Switches Glossar der Begriffe

Ziel

Dieser Artikel enthält eine Liste der Begriffe, die bei der Einrichtung, Konfiguration und Fehlerbehebung von Cisco Small Business Switches verwendet werden.

Unterstützte Geräte

Sx200-Serie

Sx250-Serie

Sx300-Serie

Sx350-Serie

SG300X-Serie

Sx500-Serie

Sx550X-Serie

Liste der Begriffe

802.1X-Komponente - Komponente ist eine der drei Funktionen des 802.1X IEEE-Standards. 802.1X wurde entwickelt, um Sicherheit in Layer 2 des OSI-Modells bereitzustellen. Sie besteht aus den folgenden Komponenten: Supplicant, Authenticator und Authentication Server. Ein Supplicant ist der Client oder die Software, der bzw. die eine Verbindung mit einem Netzwerk herstellt, um auf Ressourcen in diesem Netzwerk zugreifen zu können. Es muss Anmeldeinformationen oder Zertifikate bereitstellen, um eine IP-Adresse zu erhalten und Teil dieses speziellen Netzwerks zu sein. Ein Supplicant kann erst auf die Netzwerkressourcen zugreifen, wenn er authentifiziert wurde.

ACL - Eine Zugriffskontrollliste (ACL) ist eine Liste von Netzwerkverkehrsfiltern und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert bestimmte Ressourcen oder ermöglicht ihnen den Zugriff darauf. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät erlaubt oder verweigert wird. Der Router oder Switch überprüft jedes Paket, um anhand der in den Zugriffslisten festgelegten Kriterien zu bestimmen, ob das Paket weitergeleitet oder verworfen werden soll. Zugriffslistenkriterien können die Quelladresse des Datenverkehrs, die Zieladresse des Datenverkehrs, das Upper-Layer-Protokoll oder andere Informationen sein.

IGMP-Snooping - Internet Group Management Protocol (IGMP) ist ein Protokoll, das auf Switches ausgeführt wird und diese in die Lage versetzt, Multicast-Datenverkehr dynamisch zu erfassen. IGMP-Snooping ist eine Funktion, mit der ein Netzwerk-Switch IGMP-Konversationen zwischen Hosts und Routern abhören kann. IGMP-Snooping führt einen Filtermechanismus aus, der im Router aktiviert ist, um den Multicast-Verkehr einer Gruppe nur an die Ports weiterzuleiten, die der Gruppe beigetreten sind. IGMP-Snooping reduziert den Datenverkehr im Netzwerk und steigert die Leistung der Hosts hinter dem Router. Multicasts können von den Links gefiltert werden, die sie nicht benötigen.

IPv4 - IPv4 ist ein 32-Bit-Adressierungssystem zur Identifizierung eines Geräts in einem Netzwerk. Es ist das Adressierungssystem, das in den meisten Computernetzwerken, einschließlich des Internets, verwendet wird.

IPv6 - IPv6 ist ein 128-Bit-Adressierungssystem zur Identifizierung eines Geräts in einem Netzwerk. Es ist der Nachfolger von IPv4 und die neueste Version des Adressierungssystems, das in Computernetzwerken verwendet wird. IPv6 wird derzeit weltweit eingeführt. Eine IPv6-Adresse wird in acht Hexadezimalfeldern dargestellt, die jeweils 16 Bit enthalten. Eine IPv6-Adresse ist in zwei Teile unterteilt, die jeweils 64 Bit umfassen. Der erste Teil ist die Netzwerkadresse, der zweite Teil die Hostadresse.

Link-Flap - Link-Flap ist eine Situation, in der eine physische Schnittstelle auf dem Switch dreimal pro Sekunde für eine Dauer von mindestens 10 Sekunden kontinuierlich hoch- und herunterfährt. Die häufigste Ursache ist in der Regel ein defektes, nicht unterstütztes oder nicht standardmäßiges Kabel oder SFP (Small Form-Factor Pluggable) oder andere Probleme mit der Synchronisierung von Links. Die Ursache für Link-Flapping kann intermittierend oder dauerhaft sein.

MAC-basierte ACL: MAC-basierte (Media Access Control) Zugriffskontrollliste ist eine Liste von Quell-MAC-Adressen. Wenn ein Paket von einem Wireless Access Point zu einem LAN-Port oder umgekehrt gelangt, überprüft dieses Gerät, ob die Quell-MAC-Adresse des Pakets mit einem Eintrag in dieser Liste übereinstimmt, und vergleicht die ACL-Regeln mit dem Inhalt des Frames. Anschließend werden die übereinstimmenden Ergebnisse verwendet, um dieses Paket zuzulassen oder abzulehnen. Pakete vom LAN- zum LAN-Port werden jedoch nicht überprüft.

MLD-Snooping - Multicast ist die Technik der Netzwerkschicht, die Datenpakete von einem Host an die ausgewählten Hosts in einer Gruppe überträgt. Auf der unteren Ebene überträgt der Switch den Multicast-Verkehr auf alle Ports, selbst wenn nur ein Host ihn empfangen möchte. Multicast Listener Discovery (MLD) Snooping wird verwendet, um IPv6-Multicast-Datenverkehr nur an die gewünschten Hosts weiterzuleiten. Wenn MLD-Snooping auf dem Switch aktiviert ist, werden die MLD-Nachrichten erkannt, die zwischen dem IPv6-Router und den an die Schnittstelle angeschlossenen Multicast-Hosts ausgetauscht werden. Anschließend wird eine Tabelle verwaltet, die den IPv6-Multicast-Verkehr beschränkt und dynamisch an die Ports weiterleitet, die ihn empfangen möchten.

MSTP - Multiple Spanning Tree Protocol (MSTP) ist ein Protokoll, das mehrere Spanning Trees (Instanzen) für jedes virtuelle LAN (VLAN) in einem einzelnen physischen Netzwerk erstellt. Dadurch verfügt jedes VLAN über eine konfigurierte Root-Bridge und Weiterleitungstopologie. Dadurch wird die Anzahl der Bridge Protocol Data Units (BPDUs) im

Netzwerk reduziert und die Belastung der zentralen Verarbeitungseinheiten (CPUs) der Netzwerkgeräte reduziert.

Port-/VLAN-Spiegelung - Die Spiegelung ist eine Methode zur Überwachung des Netzwerkverkehrs. Mit der Port- oder VLAN-Spiegelung werden Kopien von ein- und ausgehenden Paketen an den Ports (Quell-Ports) eines Netzwerkgeräts an einen anderen Port (Ziel-Port) weitergeleitet, wo die Pakete untersucht werden. Diese wird vom Netzwerkadministrator als Diagnosetool verwendet.

Port-Sicherheit - Die Konfiguration der Port-Sicherheit ist eine Möglichkeit, die Netzwerksicherheit zu verbessern. Sie kann auf einem bestimmten Port oder einer Link Aggregation Group (LAG) konfiguriert werden. Eine LAG kombiniert einzelne Schnittstellen in einer einzelnen logischen Verbindung, wodurch eine aggregierte Bandbreite von bis zu acht physischen Verbindungen bereitgestellt wird. Sie können den Zugriff für verschiedene Benutzer an einem bestimmten Port/einer bestimmten LAG einschränken oder zulassen. Port-Sicherheit kann auch mit dynamisch abgefragten und statischen MAC-Adressen verwendet werden, um den eingehenden Datenverkehr eines Ports zu begrenzen.

Protokollbasiertes VLAN - Protokollbasierte Gruppen können definiert und an einen Port gebunden werden. Daher wird jedes Paket, das von den Protokollgruppen stammt, dem konfigurierten VLAN auf der Seite zugewiesen. Das protokollbasierte VLAN unterteilt das physische Netzwerk für jedes erforderliche Protokoll in logische VLAN-Gruppen. Im eingehenden Paket wird der Frame überprüft, und die VLAN-Mitgliedschaft kann anhand des Protokolltyps bestimmt werden. Die Zuordnung von protokollbasierten Gruppen zu VLANs erleichtert die Zuordnung einer Protokollgruppe zu einem einzelnen Port.

QoS - Quality of Service (QoS) ermöglicht die Priorisierung des Datenverkehrs für verschiedene Anwendungen, Benutzer oder Datenflüsse. Es kann auch verwendet werden, um eine Leistung auf einem bestimmten Niveau zu garantieren, wodurch die Servicequalität des Kunden beeinflusst wird. Die QoS wird im Allgemeinen von den folgenden Faktoren beeinflusst: Jitter, Latenz und Paketverlust.

RADIUS-Server - RADIUS (Remote Authentication Dial-In User Service) ist ein Authentifizierungsmechanismus für Geräte, die eine Verbindung mit einem Netzwerkdienst herstellen und diesen verwenden. Es wird für zentralisierte Authentifizierungs-, Autorisierungs- und Abrechnungszwecke verwendet. Ein RADIUS-Server steuert den Zugriff auf das Netzwerk, indem er die Identität der Benutzer anhand der eingegebenen Anmeldedaten überprüft. Beispielsweise wird ein öffentliches Wi-Fi-Netzwerk auf einem Universitätscampus installiert. Nur Studenten mit einem Kennwort können auf diese Netzwerke zugreifen. Der RADIUS-Server überprüft die von den Benutzern eingegebenen Kennwörter und gewährt bzw. verweigert den Zugriff.

RSTP: Rapid Spanning Tree Protocol (RSTP) ist eine Erweiterung von STP. RSTP bietet eine schnellere Spanning Tree-Konvergenz nach einer Topologieänderung. STP kann 30 bis 50 Sekunden in Anspruch nehmen, um auf eine Topologieänderung zu reagieren, während RSTP innerhalb des Dreifachen der konfigurierten Hello-Zeit antwortet. Das RSTP ist abwärtskompatibel mit dem STP.

SNMP - Simple Network Management Protocol (SNMP) ist ein Netzwerkstandard zum Speichern und Austauschen von Informationen über Netzwerkgeräte. SNMP vereinfacht die Netzwerkverwaltung, Fehlerbehebung und Wartung.

Spanning Tree: Spanning Tree Protocol (STP) ist ein Netzwerkprotokoll, das in einem Local Area Network (LAN) verwendet wird. STP soll eine schleifenfreie Topologie für ein LAN sicherstellen. STP entfernt Schleifen durch einen Algorithmus, der sicherstellt, dass nur ein aktiver Pfad zwischen zwei Netzwerkgeräten vorhanden ist. STP stellt sicher, dass der Datenverkehr den kürzestmöglichen Pfad innerhalb des Netzwerks wählt. STP kann redundante Pfade auch automatisch wieder als Backup-Pfade aktivieren, wenn ein aktiver Pfad ausfällt.

SSL-Server - Secure Sockets Layer (SSL) ist ein Protokoll, das hauptsächlich für das Sicherheitsmanagement im Internet verwendet wird. Es verwendet eine Programmschicht, die sich zwischen der HTTP- und der TCP-Schicht befindet. Für die Authentifizierung verwendet SSL Zertifikate, die digital signiert und an den öffentlichen Schlüssel gebunden sind, um den Besitzer des privaten Schlüssels zu identifizieren. Diese Authentifizierung hilft während der Verbindungszeit. Durch die Verwendung von SSL werden die Zertifikate während des Authentifizierungsprozesses in Blöcken ausgetauscht, die in dem im ITU-T-Standard X.509 beschriebenen Format vorliegen. Anschließend werden von der externen Zertifizierungsstelle X.509-Zertifikate ausgestellt, die digital signiert werden.

Syslog-Aggregation - Ein Syslog-Dienst akzeptiert Nachrichten und speichert sie in Dateien oder druckt sie entsprechend einer einfachen Konfigurationsdatei. Syslog-Aggregation bedeutet, dass mehrere Syslog-Meldungen desselben Typs nicht bei jedem Auftreten einer Instanz angezeigt werden. Wenn Sie die Protokollierungsaggregation aktivieren, können Sie die Systemmeldungen filtern, die Sie für einen bestimmten Zeitraum erhalten. Er erfasst einige Syslog-Meldungen desselben Typs, sodass sie nicht sofort, sondern in einem bestimmten Intervall angezeigt werden.

TACACS+ (Terminal Access Controller Access Control System) (TACACS+) ist ein proprietäres Protokoll von Cisco, das zur Implementierung erweiterter Sicherheit verwendet wird, indem Authentifizierung und Autorisierung über Benutzername und Kennwort erfolgt. Um einen TACACS+-Server zu konfigurieren, muss der Benutzer über die Berechtigung 15 verfügen, die ihm Zugriff auf alle Konfigurationsfunktionen des Switches gewährt. Einige Switches können als TACACS+-Client fungieren, wobei alle verbundenen Benutzer über einen ordnungsgemäß konfigurierten TACACS+-Server im Netzwerk authentifiziert und autorisiert werden können. TACACS+ unterstützt nur IPv4.

TFTP-Server - Ein Trivial File Transfer Protocol (TFTP)-Server ist ein Server, der zum automatischen Übertragen von Konfigurations- und Startdateien zwischen Geräten in einem LAN verwendet wird. Das Protokoll ist einfach und ermöglicht eine geringe Speichernutzung. Diese Einfachheit ermöglicht jedoch auch eine leichte Kompromittierung des Protokolls. Aus diesem Grund wird TFTP nur selten mit dem Internet verwendet.

VLAN - Ein Virtual Local Area Network (VLAN) ist ein Switch-Netzwerk, das unabhängig von den physischen Standorten der Benutzer logisch nach Funktion, Bereich oder Anwendung segmentiert ist. VLANs sind eine Gruppe von Hosts oder Ports, die sich an beliebiger Stelle in einem Netzwerk befinden können, aber so kommunizieren, als befänden sie sich in

demselben physischen Segment. VLANs vereinfachen das Netzwerkmanagement, indem Sie ein Gerät in ein neues VLAN verschieben können, ohne die physischen Verbindungen zu ändern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.